## **Binding certificates for distributed installations**

These instructions are applied when SQLDM and Dashboard are installed on different servers. They are the continuation of the Resolving Dashboard certificate error message, which means the Dashboard certificate was already created.



If you have not installed KeyStore Explorer, download it, and install the application.

## Dashboard and SQL Diagnostic Manager installed on different machines

This scenario considers that both products are installed on different servers:

- Dashboard is installed and is being accessed on Server 1.
- SQLDM Services are installed on Server 2.

Once your Dashboard certificate is created on Server 1, follow the steps below

1. Open the Microsoft Management Console (MMC) by selecting Run from the Start menu, enter "mmc", and click OK.

🖅 Run	×
٨	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	mmc ~
	OK Cancel <u>B</u> rowse

- 2. When the MMC window opens, click File from the menu toolbar, and select Add/Remove Snap-in...
- 3. The Add or Remove Snap-ins window opens, Add Certificates, and click OK.
- 4. Configure the steps of the Certificate snap-in wizard, and click Finish.
- 5. Close the Add or Remove Snap-in window by clicking  $\ensuremath{\text{OK}}$  .

## 6. Expand Certificates, right-click the Personal folder, select All Tasks, and click Import...

a Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates] -							
🚰 File Action View Fa	vorites Window Help						_ & ×
🗢 🄿 🖄 📅 📋 🧟	🗟 🔽 📻						
📔 Console Root	Issued To		Issued By	Actions			
Certificates (Local Cor	🕼 Idera	a Inc	Idera Inc		Certificates	<b>_</b>	
Certificates		🙄 local	alhost	localhost		More Actions	+
V 📫 Trusted Root Ce	All Tasks	>	Request New Certific	ate	al		
Certificates	View	>	Import		al		
> 📔 Enterprise Trust	New Window from Here	Advanced Operations >					
> Trusted Publish	New Testined View						
> 📔 Untrusted Certi –	New laskpad view						
> 📔 Third-Party Roc	Refresh						
> Trusted People	Export List						
> Preview Build R	Help						
> 🧮 Test Roots							
> 🚆 AAD Token Issuer							
> eSIM Certification							
Delvi esilvi Certific	ation Authorities Roots						
> 📔 Remote Desktop							
> 📔 Certificate Enrollm	nent Requests						
Contains actions that can be r	performed on the item						

- 7. Import the .cer certificate under the Trusted Root Certificate Authorities folder on Server 2.
- 8. Import the .pfx certificate under the Personal folder on Server 2.
- 9. Retrieve the thumbprint of the imported PFX key.
  - a. Double-click the imported PFX key.
    - b. On the Certificate window, go to the Details tab.
    - c. Scroll down and click Thumbprint. You need to copy the characters from the box.

If the thumbprint has extra spaces between the hexadecimal numbers, remove them. For example, the thumbprint ""a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b" should be edited to ""a909502dd82ae41433e6f83886b00d 4277a32a7b".

- 10. Follow these last steps to bind the new PFX key by using the commands below:
  - a. Open CMD as an Administrator and execute the following command to delete existing bindings to the IDERA SQL Diagnostic Manager Rest Service on <u>Server 2</u>:

netsh http delete ssl 0.0.0.0:5171

b. Bind the PFX key by using the following command in an elevated command prompt session on <u>Server 2</u>, GUID SQLDM: 0051d7ed-de72-46d3-ae44-97d566b1ca5a

```
netsh
http
add sslcert ipport=0.0.0.0:5171 certhash="<PFX key's thumbprint>" appid="{0051d7ed-de72-46d3-
ae44-97d566blca5a}" clientcertnegotiation=enable
// Remove the spaces from the PFX Key's thumbprint
```

## IDERA | Products | Purchase | Support | Community | Resources | About Us | Legal